3. Publicznoprawne aspekty bezpieczeństwa danych osobowych w szkołach wyższych w Polsce

Agnieszka Bednarczyk

Wprowadzenie

Zakres zbieranych przez różnorakie instytucje, przedsiębiorstwa i organy państwa danych osobowych nieustannie się zmienia i poszerza. Dane te gromadzone i przetwarzane są w celach handlowych, społecznych, kulturalnych, ale także w celu realizowania zadań przez państwo. W związku z tym istnieje ryzyko przekroczenia uprawnień do zbierania i przetwarzania tych danych zarówno przez podmioty publiczne, jak i prywatne oraz zbyt inwazyjne wkraczanie w sferę prywatności obywateli, co w konsekwencji może prowadzić do naruszenia ich dóbr osobistych i prawa do prywatności. Rozwój praw człowieka do ochrony jego danych osobowych rozpoczął się wraz z erą informatyczną[1]. Komputeryzacja i cyfryzacja zbieranych danych umożliwiły bowiem ich łatwiejsze i szybsze przetwarzanie oraz przechowywanie. Aby zarówno jednostka, której dane dotyczą, jak i podmioty zbierające i przetwarzające te dane posiadały kontrolę nad gromadzonymi informacjami, konieczna w tym celu jest pełna regulacja prawna obligująca te podmioty do wprowadzania procedur zapewniających bezpieczeństwo tworzonych zbiorów danych. Niniejsze opracowanie ma na celu przedstawienie sposobów i wymagań prawnych związanych z ochroną danych osobowych w szkołach wyższych w Polsce.

3.1. Geneza ochrony danych osobowych

Obowiązek zabezpieczania i ochrony danych osobowych wywieść należy z Konwencji nr 108 Rady Europy w dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[2]. Postanowienia Konwencji dotyczyły sfery publicznoprawnej, w której działają także

[1] M.T. Tinnefeld, *Ochrona danych osobowych – kamień węgielny budowy Europy,* [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 35.

[2] Dz.U. z 2003 r., Nr 3, poz. 25 – zwana dalej Konwencją; Konwencja weszła w życie 1 października 1985 r., po ratyfikowaniu jej przez 5 państw. Polska ratyfikowała Konwencję 24 kwietnia 2002 r., a weszła ona w życie 1 września 2002 r.

szkoły wyższe, nie wywołując bezpośrednich skutków prawnych po stronie obywateli państw Konwencji. Zgodnie z art. 1 Konwencji każdy obywatel państw członkowskich Rady Europy może oczekiwać od władz danego państwa ochrony jego praw i wolności, w szczególności prawa do poszanowania sfery osobistej, w związku z automatycznym przetwarzaniem danych osobowych. Zasada minimum, ochrony danych osobowych została wyrażona w art. 4 Konwencji. Ratyfikując Konwencję, każdy kraj będący jej stroną zobowiązuje się do wprowadzenia do prawa wewnętrznego przepisów koniecznych dla realizacji ochrony danych osobowych. Na gruncie przepisów Konwencji za podstawowe zasady ochrony danych osobowych uznano: zasadę adekwatności danych, zasadę związania celem zbierania danych, zasadę odpowiedniego zabezpieczania danych, zasadę respektowania uprawnień informacyjnych osób, których dane dotyczą. Na gruncie niniejszej Konwencji przyjęta została także dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tychże danych[3]. Dyrektywa jako akt prawa wtórnego Unii Europejskiej wiąże państwa członkowskie (podobnie jak Konwencja) w odniesieniu do rezultatu, jednak pozostawia organom krajowym swobodę wyboru formy i środków zmierzających do osiągnięcia tego rezultatu[4]. W dyrektywie wyszczególnione zostały podstawowe zasady przetwarzania danych, których przestrzeganie ma zapewnić bezpieczeństwo przetwarzanych danych. Za najważniejszą z zasad uznano wymóg rzetelnego i zgodnego z prawem przetwarzania danych osobowych. Jako kolejne zasady gwarantujące bezpieczeństwo danych i poszanowanie praw osób, których dane dotyczą, uznano: zasadę celowości przetwarzania danych, zasadę adekwatności przetwarzania danych, zasadę poprawności merytorycznej danych, zasadę ograniczania czasowego przetwarzania danych, zasadę poszanowania praw osób fizycznych przy przetwarzaniu ich danych osobowych, zasadę stosowania odpowiednich środków zabezpieczenia danych, zakaz przekazywania danych osobowych poza teren Europejskiego Obszaru Gospodarczego (poza wyjątkami przewidzianymi w dyrektywie)[5]. Wprowadzenie jednolitej ochrony danych osobowych w państwach Unii miało i ma na celu zapewnienie swobodnego przepływu towarów, usług i osób na terenie wspólnoty[6].

[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tychże danych, Dz.Urz. L 281 z dnia 23 listopada 1995 r. – zwana dalej dyrektywą.

[4] S. Biernat, *Prawo Unii Europejskiej a prawo państw członkowskich*, [w:] *Prawo Unii Europejskiej*, red. J. Barcz, Warszawa 2004, s. 212.

[5] Przepisy rozdziału II sekcji I dyrektywy.

[6] Preambuła do dyrektywy 95/46/WE.

W polskim prawie podstaw ochrony danych osobowych należy upatrywać w przepisach Konstytucji RP[7]. W art. 47 Konstytucji zostało zagwarantowane prawo do ochrony życia prywatnego, rodzinnego, czci, dobrego imienia oraz decydowania o swoim życiu osobistym. W art. 51 wyszczególniono natomiast bezpośrednie gwarancje bezpieczeństwa i ochrony danych osobowych, tj. prawo każdej osoby do decydowania o ujawnieniu dotyczących jej informacji, prawo każdej osoby do sprawowania kontroli nad informacjami na swój temat, prawo dostępu do dotyczących tych osób dokumentów i zbiorów danych, prawo do weryfikacji i żądania usunięcia danych osobowych. Konkretyzacją konstytucyjnych uregulowań stała się Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Ustawa ta nie przejęła jednak wprost z dyrektywy rozdziału dotyczącego zasad przetwarzania danych osobowych. Zostało to uregulowane w samym zakresie obowiązywania ustawy. Przepisy ustawy opisują bowiem zasady i tryb postępowania przy przetwarzaniu danych osobowych prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach oraz zakres działania, zasady organizacji i funkcjonowania Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

Jest wiele powodów, dla których zapewnienie bezpieczeństwa gromadzenia i przetwarzania danych osobowych jest tematyką na tyle istotną, aby regulować ją w sposób ustawowy. Do najważniejszych z nich można zaliczyć w pierwszej kolejności gromadzenie danych w większe i mniejsze zbiory. Zbiory w dzisiejszych czasach praktycznie w całości zapisywane i utrwalane są w formie systemów komputerowych, dzięki którym możliwe jest nie tylko szybkie przeszukiwanie, uaktualnianie i przetwarzanie tych informacji, ale także dużo łatwiejsze ich udostępnianie oraz tworzenie zbiorów o ogromnych rozmiarach. W tak zorganizowanych bazach danych osobowych znacznie wzrasta ryzyko zaistnienia naruszeń. Ze względu na duże możliwości techniczne widoczna staje się waga właściwych rozwiązań prawnych w tym zakresie. Brak uregulowań może prowadzić bowiem do niedozwolonego ingerowania w szeroko rozumianą wolność osobistą i prywatność jednostek, pozbawić ich możliwości kontrolowania i ingerowania w zakres gromadzonych na ich temat danych, a także decydowania, komu mogą zostać udostępnione[8]. Kolejnym powodem konieczności prawidłowego zabezpieczania danych osobowych jest udostępnianie danych i ich przetwarzanie za pomocą sieci komputerowych. Obecne stosunki handlowe, ekonomiczne, polityczne

[7] Konstytucja Rzeczypospolitej Polskiej z 1997 r., Dz.U. Nr 78, poz. 483.

[8] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, wyd. Wolters Kluwer, Kraków 2007, s. 51.

czy społeczne realizowane są w ogromnej mierze za pośrednictwem internetu. Pomimo wielu zalet, które niesie za sobą taki sposób wykorzystywania globalnej sieci, otwiera on również wiele pól, na których może dojść do niepożądanej ingerencji w gromadzone dane z zewnątrz, ich kopiowania, przejmowania i wykorzystywania sprzecznie z celem, dla którego zostały zgromadzone, a przede wszystkim bez zgodny osób, których dotyczą.

Przepisy o ochronie danych osobowych mają zapewnić procedury niezbędne do zabezpieczenia podstawowych praw i wolności, zwłaszcza prawa do prywatności oraz niezbędną bazę dla działania podmiotów prywatnych i publicznych.

3.2. Uprawnienie organów uczelni do przetwarzania danych osobowych

Ustawa o ochronie danych osobowych z zamysłu ustawodawcy w sposób kompleksowy reguluje przetwarzanie danych osobowych zarówno przez podmioty publiczne, jak i podmioty sektora prywatnego[9]. Zakres obowiązywania niniejszej ustawy obejmuje również działania organów szkół wyższych, związanych z gromadzeniem i przetwarzaniem danych studentów w ramach realizacji swoich celów, a także w ramach prowadzonych w uczelniach postępowań administracyjnych. Sama ustawa o szkolnictwie wyższym[10] nie reguluje wprost kwestii związanych z ochroną danych osobowych. W tym zakresie należy się posługiwać bezpośrednio ustawą o ochronie danych osobowych. Aby zapewnić ochronę danych osobowych przetwarzanych przez podmioty takie jak uczelnie[11] na gruncie art. 3 ustawy zobowiązano podmioty publiczne oraz podmioty niepubliczne wykonujące zadania powierzone przez państwo do stosowania przepisów ustawy o ochronie danych osobowych, w przypadku spełnienia łącznie dwóch warunków, tj. zadanie realizowane przez dany podmiot musi należeć do sfery publicznoprawnej, realizacja zadań publicznoprawnych musi wynikać z przepisów ustawowych. W przypadku wykonywania przez podmioty prywatne zadań, które można uznać za zadania publiczne, jednakże niezastrzeżonych ustawowo do kompetencji konkretnych typów podmiotów, tzn. zadań, które mogą być wyko-

[9] § 1 ustawy.

[10] Ustawa z dnia 27 lipca 2005 r. – Prawo o szkolnictwie wyższym, Dz.U. 2005 Nr 164, poz. 1365 z późn. zm.

[11] Zaliczyć do tej kategorii można również choćby przedszkola, niepubliczne zakłady opieki zdrowotnej, szkoły.

nywane przez dowolne podmioty prowadzące działalność gospodarczą, nie przesądza o konieczności stosowania zapisów ustawy[12]. W przypadku uczelni warunek realizowania zadań publicznych zostaje spełniony na mocy zapisów art. 4 ust. 3 Ustawy o szkolnictwie wyższym, zgodnie z którym uczelnie w swojej misji stanowią część narodowego systemu edukacji i nauki, a co za tym idzie: wykonują zadania zastrzeżone dla państwa. Obowiązek wykonywania przez uczelnie zadań powierzonych przez państwo wynika także z art. 18 i 20 tejże ustawy. Co więcej, zadania te nie są dostępne dla wszystkich podmiotów prowadzących działalność gospodarczą, a jedynie dla tych, które jak w przypadku uczelni publicznych zostaną powołane specjalnie w tym celu na mocy aktu ustawowego[13], a w przypadku uczelni niepublicznych ich działalność odbywa się na mocy pozwolenia wydawanego przez Ministra Nauki i Szkolnictwa Wyższego, w drodze decyzji administracyjnej[14].

Danymi osobowymi w szkołach wyższych zarządza rektor, pełniąc w tym zakresie funkcję administratora danych osobowych gromadzonych w uczelni. Uprawnienie rektora w tym zakresie wywieść należy z art. 66 Ustawy o szkolnictwie wyższym, zgodnie z którym rektor kieruje działalnością uczelni i reprezentuje ją na zewnątrz, w połączeniu z art. 7 Ustawy o ochronie danych osobowych. Art. 7 ustawy zawiera definicję instytucji administratora danych osobowych. Administratorem danych osobowych jest organ, jednostka organizacyjna, podmiot lub osoba spełniająca warunki polegające na wykonywaniu zadań publicznych lub w przypadku osoby fizycznej lub prawnej prowadzenia działalności zarobkowej, decyduje o celach i środkach przetwarzania danych.

Obowiązki rektora jako administratora danych to: udostępnianie danych osobom, których dane dotyczą zawartych w zbiorach informacji, w celu ich uaktualniania lub zmiany, obowiązek rejestracyjny zbiorów danych, zabezpieczanie danych, zachowywanie ich poufności, integralności i nienaruszalności. Administrator danych odpowiada za legalność przetwarzania danych i ich bezpieczeństwo. Rektor, gromadząc i przetwarzając dane, nie czyni tego osobiście. Osoby, które wykonują polecenia rektora w zakresie przetwarzania powierzonych uczelni danych osobowych, muszą posiadać w tym zakresie specjalne umocowanie[15]. Upoważnienie wymagane jest nawet w przypadku, gdy do zakresu obowiązków na danym stanowisku należy przetwarzanie danych. Oprócz tych osób w szkołach wyższych odrębne upoważnienia powinni również posiadać:

[12] P. Litwiński, *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, Wolters Kluwer, Warszawa 2009, s. 36.

[13] Ustawa o szkolnictwie wyższym, art. 18.

[14] *Ibidem*, art. 20.

[15] Ustawa o ochronie danych osobowych, art. 31.

- kierownicy poszczególnych jednostek organizacyjnych – dziekani i prodziekani w stosunku do przetwarzania danych osobowych studentów na właściwych im wydziałach,
- pracownicy zatrudnieni na stanowiskach księgowych – w zakresie realizowanych zadań,
- pracownicy pionu informatyki, szczególnie administrator systemu informatycznego i pracownik pełniący funkcję administratora bezpieczeństwa informacji,
- uczniowie i praktykanci, jeżeli odbywanie praktyki może się wiązać z przetwarzaniem danych osobowych;
- pracownicy administracyjni, jeżeli w zakresie ich obowiązków leży praca z danymi osobowymi[16].

Formalne upoważnienie do dostępu do danych osobowych przetwarzanych w danej uczelni powinny otrzymać również prorektorzy, zwłaszcza prorektorzy ds. studenckich.

Wyżej wymienione osoby (poza administratorem bezpieczeństwa danych i administratorem systemu informatycznego) nie posiadają przymiotu administratora danych i nie ponoszą bezpośredniej odpowiedzialności za prawidłowość przetwarzania i zabezpieczania danych przed Generalnym Inspektorem Ochrony Danych Osobowych[17]. Upoważnieni pracownicy obowiązani są działać w granicach prawa i polityki bezpieczeństwa wypracowanej w danej uczelni. Ciąży na nich również tajemnica danych oraz sposobów ich zabezpieczania. Pracownicy o wiążącej ich tajemnicy powinni zostać poinformowani w chwili nadania im upoważnienia do przetwarzania danych. Można powiedzieć, że jest to forma tajemnicy zawodowej, zwłaszcza gdy osoby przetwarzające dane czynią to na podstawie umowy o pracę. Obowiązek zachowania danych osobowych w tajemnicy oznacza zakaz ujawniania danych studentów innym osobom. Naruszenie tego obowiązku prowadzi do odpowiedzialności karnej[18].

Na gruncie Ustawy o szkolnictwie wyższym oraz Ustawy o ochronie danych administratorem danych jest nie tylko rektor, ale także administrator bezpieczeństwa informacji (ABI), którego wyznacza administrator ochrony danych osobowych[19]. Obowiązek wyznaczenia ABI dotyczy nie tylko tych podmiotów, które przetwarzają dane w systemach informatycznych, ale tak-

[16] J. Borowicz, *Obowiązek prowadzenia przez pracodawcę dokumentacji osobowej i organizacyjnej z zakresu ochrony danych osobowych. Teza nr 3*, PiZS.2001.3.2, LEX 29032/3.

[17] Ustawa o ochronie danych osobowych, art. 8.

[18] *Ibidem*, art. 51.

[19] Ustawa o ochronie danych osobowych, art. 36 ust. 3

że w przypadku przetwarzania danych ręcznie. Ustawa nie precyzuje jednak szczegółowego zakresu obowiązków ABI. Jego głównym zadaniem jest nadzorowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych[20], przede wszystkim zabezpieczanie danych tak, aby nie zostały one udostępnione osobom nieupoważnionym, nie były przetwarzane z naruszeniem ustawy, kontrolowanie kwestii związanych z ich zmianą, uszkodzeniem lub zniszczeniem. Zazwyczaj w uczelniach funkcję ABI pełni pracownik administracyjny uczelni, który zostaje wyposażony w kompetencje nadzorcze i możliwość ingerowania w gromadzone zbiory, a także kompetencje uprawniające do wydawania wiążących wytycznych związanych z przetwarzaniem danych. Wyznaczenie ABI następuje w formie pisemnej. Niejednokrotnie funkcja ABI w uczelniach łączona jest z funkcją ASI, czyli administratora systemu informatycznego. Dzieje się tak ze względu na komputeryzację danych gromadzonych w uczelniach. Ilość danych, które uczelnie obowiązane są gromadzić na temat swoich studentów, wyklucza bowiem możliwość ręcznego przetwarzania tych danych, wymuszając stosowanie rozwiązań systemów informatycznych. Zarządzanie tak zorganizowanym systemem danych, zwłaszcza w kontekście ich ochrony i możliwości szybkiej ingerencji administratora w ich zakres w sytuacji zaistnienia naruszeń przemawia na gruncie szkół wyższych za łączeniem tych funkcji.

3.3. Bezpieczeństwo i ochrona danych osobowych w szkołach wyższych

Definicje

Szkoły wyższe w Polsce gromadzą i przetwarzają dane osobowe studentów i kandydatów na studia w celu wykonywania swoich zadań. Głównym i najważniejszym zadaniem uczelni jest zgodnie z art. 6 Ustawy o szkolnictwie wyższym prowadzenie studiów. W tym właśnie celu gromadzone są dane studentów, które wykorzystywane są później przez organy uczelni do realizowania procesu kształcenia oraz prowadzenia postępowania administracyjnego w sprawach studentów. Przed omówieniem kwestii bezpieczeństwa danych osobowych w uczelniach należy odpowiedzieć na dwa pytania: czym są dane osobowe i zbiory danych.

Definicję danych osobowych zawiera art. 6 o ochronie danych osobowych. Zgodnie z jego treścią za dane osobowe uważa się wszelkie informacje

[20] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych…*, s. 609.

dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się natomiast za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Za dane osobowe można uznać na tej podstawie „wszelkie informacje" odnoszące się do każdego aspektu osoby, jej stosunków osobistych i rzeczowych, jej życia zawodowego, prywatnego, wykształcenia, wiedzy czy cech charakteru. Danymi osobowymi są zarówno informacje już rozpowszechnione lub opublikowane (zamieszczone w publikowanych materiałach), jak i w ogóle jeszcze nieujawnione[21]. Aby określoną informację można było zaliczyć do danych osobowych, muszą zostać spełnione dwa warunki: dane muszą dotyczyć osoby fizycznej, a jej tożsamość musi być na ich podstawie możliwa do ustalenia. Zgodnie z tym za dane osobowe nie można uznać danych dotyczących jednostek organizacyjnych (bez względu na to, czy posiadają one osobowość prawną, czy nie) ani szeroko rozumianych organów administracji państwowej. W polskim reżimie prawnym kwestie dotyczące podmiotów innych niż osoby fizyczne regulowane są przez odrębne ustawy. Aby dana informacja mogła zostać uznana za „dotyczącą osoby fizycznej", musi przekazywać informacje, które w jakikolwiek sposób odnoszą się do zidentyfikowanej bądź możliwej do zidentyfikowania osoby fizycznej, a identyfikacja odbywa się na podstawie całokształtu posiadanych informacji[22]. W tym kontekście do danych osobowych można również zaliczyć informację nieprzynależącą do zbioru danych, ale która w połączeniu z informacjami znajdującymi się w zbiorze umożliwia zidentyfikowanie osoby fizycznej[23]. Idąc tym tokiem rozumowania, za dane osobowe należy uznać nie tylko nazwiska czy daty urodzenia, ale także zainteresowania czy kierunek odbywanych studiów. Wyłączenia spośród tej grupy należy dokonać w stosunku do danych dotyczących stosunków majątkowych[24]. Zgodnie z przytoczonym orzeczeniem ujawnienie osobie trzeciej danych dotyczących wysokości wynagrodzenia za pracę pracownika nie stanowi samo w sobie naruszenia prywatności. Jeżeli natomiast taka informacja ujawniała-

[21] *Ibidem*, s. 346.

[22] *Ibidem*, s. 351.

[23] A. Bierć, *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce – aspekty cywilnoprawne*, [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, red. P. Fajgielski, Lublin 2008, s. 121–122.

[24] Uchwała składu 7 sędziów SN z dnia 16 lipca 1993 r., I PZP 28/93, OSNC 1994, nr 1, poz. 2.

by obowiązki alimentacyjne pracownika, można już mówić o naruszeniu jego praw i tajemnicy danych osobowych. Poza już wymienionymi przykładami danych osobowych należy wskazać numer powszechnego elektronicznego systemu ewidencji ludności (PESEL); numer identyfikacji podatkowej (NIP), numer dokumentu tożsamości (dowodu osobistego oraz paszportu), a także: wygląd zewnętrzny, wzór siatkówki oka (cechy fizyczne); struktura kodu genetycznego, grupa krwi (cechy fizjologiczne); pochodzenie, poglądy polityczne, przekonania religijne lub filozoficzne oraz przynależność wyznaniowa, partyjna lub związkowa (cechy te można zaliczyć do cech umysłowych, kulturowych lub społecznych, w zależności od sposobu interpretacji tych pojęć). Wskazane powyżej czynniki nie wyczerpują otwartego katalogu rodzajów informacji, które mogą być przypisane konkretnej osobie fizycznej[25]. W szkołach wyższych poza danymi wymienionymi powyżej za dane osobowe podlegające ochronie uznaje się dane o: punktach ECTS, kierunkach studiów podjętych przez studenta, dacie skreślenia i przyjęcia na studia, stopniu i formie studiów, studiowaniu na kolejnych kierunkach studiów, rodzaj pobieranych świadczeń pomocy materialnej[26].

Obok pojęcia danych osobowych kluczowa dla stosowania Ustawy o ochronie danych osobowych jest definicja pojęcia „zbioru danych". Pojęcie to jest znaczące w kontekście bezpieczeństwa i ochrony danych, gdyż od tego, czy zestawienie danych jest zbiorem, czy też nie, zależy powstanie obowiązku rejestracji zbioru. W przypadku gdy grupie danych osobowych nie można przypisać cech zbioru, dane takie nie podlegają zgłoszeniu do GIODO[27], który prowadzi rejestr. Za zbiór danych uznaje się posiadający pewną strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, bez względu na to, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie[28]. Aby zestaw danych

[25] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych…*, s. 356.

[26] Art. § 2 Rozporządzenia Ministra Nauki i Szkolnictwa Wyższego w sprawie danych zamieszczanych w ogólnopolskim wykazie studentów z dnia 22 września 2011 r. (Dz.U. Nr 204, poz. 1201).

[27] Art. 40. ustawy o ochronie danych osobowych: „Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Danych Osobowych (GIODO), z wyjątkiem przypadków, o których mowa w art. 43 ust. 1. Zgodnie z art. 8 ustawy o ochronie danych GIODO jest organem ochrony danych osobowych. Do jego zadań należy m.in.: kontrola zgodności przetwarzania danych z przepisami o ochronie danych osobowych, wydawanie decyzji administracyjnych i rozpatrywanie skarg w sprawach wykonywania danych osobowych, prowadzenie rejestru zbiorów danych oraz udzielanie informacji o zarejestrowanych zbiorach.

[28] Definicja wyprowadzona na podstawie art. 7 Ustawy o ochronie danych osobowych przez P. Litwińskiego, *Ochrona danych osobowych…*, s. 42.

mógł zostać uznany za zbiór danych, musi on łącznie wykazać następujące cechy: zawierać dane osobowe, posiadać zdefiniowaną własną strukturę, umożliwiać dostęp do danych według określonych kryteriów[29]. Cechą odróżniającą zbiór danych osobowych od innych zbiorów jest możliwość odnalezienia konkretnych informacji o danej osobie bez konieczności przeglądania całej zawartości zbioru. Nie wszystkie bowiem dane gromadzone w uczelniach można zdefiniować jako zbiory. Nie wyłącza to jednak stosowania przez organy uczelni przepisów dotyczących udostępniania i zabezpieczania danych studentów. Od zasady dotyczącej obowiązków rejestracji zbiorów istnieją bowiem wyjątki. Zaliczyć do nich można zbiory obejmujące dane osobowe studentów i pracowników uczelni. Zgodnie z art. 43 ust. 4 Ustawy o ochronie danych osobowych z obowiązku rejestracji zbioru zwolnieni są administratorzy danych przetwarzający dane swoich pracowników lub osób uczących się. Ustawodawca jednak nie przewidział i nie uregulował ani w Ustawie o ochronie danych osobowych, ani w Ustawie o szkolnictwie wyższym kwestii dotyczących danych osobowych kandydatów na studia i absolwentów. Powstaje zatem pytanie, czy takie zbiory podlegają zgłoszeniu, czy też nie. O ile w przypadku zbiorów danych można by pokusić się o interpretację negatywną, o tyle w przypadku zbiorów danych absolwentów sytuacja nie wydaje się już taka prosta. Zbiory danych dotyczące kandydatów mają charakter czasowy, tzn. tworzone są na potrzeby i w czasie trwania procesu rekrutacyjnego na studia, który jest stosunkowo krótki. Status studentów, którzy otrzymują decyzję pozytywną o przyjęciu na studia, zmienia się z kandydata na studenta, a ich dane osobowe zostają umieszczone w zbiorze niepodlegającym zgłoszeniu. Jeżeli natomiast kandydat otrzymuje decyzję negatywną i nie zostaje przyjęty w poczet studentów, jego dane są niszczone i nie występują w żadnym zbiorze. Brak rejestracji zbioru danych kandydatów na studia nie umniejsza ochrony zgromadzonych w nim informacji, gdyż władze uczelni muszą przestrzegać wszelkich reżimów dotyczących ochrony tych danych. Dużo bardziej skomplikowaną kwestią jest istnienie bądź nieistnienie obowiązku rejestracji zbiorów danych absolwentów. Zgodnie z art. 13a Ustawy o szkolnictwie wyższym do zadań uczelni należy monitorowanie karier zawodowych swoich absolwentów. Wiąże się to nierozerwalnie z gromadzeniem w zbiorach danych osobowych absolwentów. Przywołany przepis nie określa czasu, przez jaki uczelnia obowiązana jest zbierać dane na temat karier

[29] M. Sakowska, *Pozycja ustrojowa i zadania Generalnego Inspektora Ochrony Danych Osobowych*, „Przegląd Sejmowy" 2006, nr 2, s. 57.

zawodowych swoich absolwentów. Wiadomo jednak, że okres ten nie może być krótszy niż pięć lat. Wydawałoby się zatem, że zbiory takie podlegają zgłoszeniu, choć nigdzie nie jest to przesądzone. Janusz Barta, Paweł Fajgielski i Ryszard Markiewicz w swoim komentarzu do Ustawy o ochronie danych osobowych twierdzą, że analogicznie jak zbiory danych studentów należy potraktować zbiory danych absolwentów, korzystając z możliwości wyłączenia obowiązku rejestracyjnego[30]. Autorzy niestety bliżej nie uzasadniają swojego poglądu i nie podają przesłanek, które skłoniły ich do przyjęcia takiego stanowiska.

Zabezpieczanie danych osobowych

To, czy uczelnia przetwarza dane w zbiorze, czy też nie, o czym była już mowa wyżej, nie wpływa na ograniczenie zakresu ochrony danych osobowych studentów. Zabezpieczanie danych osobowych jest procesem mającym na celu ograniczenie prawdopodobieństwa i ryzyka wystąpienia naruszeń związanych z gromadzeniem, przetwarzaniem i udostępnianiem danych osobowych. Środki, za pomocą których zabezpieczane są dane osobowe, powinny być stosowane w dwóch etapach. Po pierwsze, przed przystąpieniem do przetwarzania danych, a po drugie, w trakcie przetwarzania danych osobowych. Środki ochrony danych mają za zadanie przeciwdziałać wszelkim zachowaniom ze strony osób trzecich, a nawet działaniu siły wyższej, zmierzającym do nieuprawnionego dostępu do danych. Środki ochrony danych powinny być stosowane nie tylko do zbiorów danych, ale do danych osobowych jako takich. Wymogi określone w art. 36 ustawy o ochronie danych odnoszą się zarówno do danych przetwarzanych w sposób manualny, jak i tych przetwarzanych w systemach informatycznych. Ustawodawca nie podaje, jakie konkretnie środki ma przedsięwziąć rektor w celu zabezpieczenia danych. Można je określić dopiero na podstawie analizy obowiązków, jakie przepisy prawa nakładają na administratora danych.

Zadaniem rektora jest zatem stosowanie skutecznych środków technicznych i organizacyjnych. Ustawodawca nie przesądza również, jakie to mają być środki. Przy stosowaniu zabezpieczeń powinno się też uwzględniać zmieniające się warunki oraz postęp techniczny (informatyczny), co może powodować konieczność zmiany czy modernizowania wprowadzonych wcześniej przez administratora systemów ochrony. Można i należy dopasowywać je do konkretnych okoliczności i warunków przetwarzania danych[31]. Zaznaczyć

[30] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych…*, s. 640.
[31] *Ibidem*, s. 607.

w tym miejscu należy, że poza zobiektywizowanymi przesłankami podjęcia takich a nie innych rodzajów ochrony danych powinna decydować także kosztochłonność wprowadzanych zabezpieczeń, charakter chronionych danych, szkodę, jaka mogłaby powstać w związku z nieuprawnionym dostępem do danych lub innym ich przetwarzaniem.

Dokumentem opisującym całość środków technicznych i organizacyjnych zapewniających ochronę danych oraz sposoby ich przetwarzania jest dokumentacja przetwarzania danych. Niezbędne elementy, jakie powinna zawierać dokumentacja, a co za tym idzie wskazówki, jakie działania powinny być podjęte w celu zabezpieczenia danych określają przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[32]. Zgodnie z § 3 rozporządzenia dokumentację powyższą stanowi: polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, które powinny być prowadzone w formie pisemnej. Na politykę bezpieczeństwa składa się:

- wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
- wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
- sposób przepływu danych pomiędzy poszczególnymi systemami,
- określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych[33].

Zacytowany katalog nie stanowi jednak katalogu zamkniętego. Powinny znaleźć się tu wszelkie informacje opisujące sposób i miejsca przetwarzania danych, a także przyjęte w tym zakresie rozwiązania techniczne i inne. Również Generalny Inspektor Ochrony Danych Osobowych posiada uprawnienia do wydawania dokumentów stanowiących pomoc dla administratorów

[32] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. z 2004 r., Nr 100, poz. 1024. – zwane dalej „rozporządzeniem".

[33] § 4 rozporządzenia.

danych osobowych. Wydaje on wytyczne w tym zakresie, w postaci poradników zamieszczanych na stronie internetowej urzędu. GIODO zdefiniował w nich pojęcie „polityka bezpieczeństwa", wskazał cel jej opracowania i wdrożenia oraz poszczególne elementy składowe tego dokumentu w sposób szerszy niż w rozporządzeniu, korzystając z otwartości zamieszczonego w nim katalogu[34]. W wytycznych oparto się m.in. na Polskiej Normie PN-ISO/IEC 17799:2007 Technika Informatyczna.

Zakres informacji, jakie powinny być zawarte w dokumencie polityki bezpieczeństwa zgodnie z Polską Normą PN-ISO/IEC 17799:2007, jest znacznie szerszy, niż przewiduje to rozporządzenie. W wytycznych wskazano, że polityka bezpieczeństwa to „zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonej organizacji". Polityka bezpieczeństwa powinna odnosić się całościowo do problemu zabezpieczenia danych osobowych u administratora danych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych. Celem polityki bezpieczeństwa jest wskazanie działań, jakie należy wykonać, oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki administratora danych w zakresie zabezpieczenia danych osobowych[35]. Zgodnie z wytycznymi zawartymi w Polskiej Normie w zakresie zarządzania bezpieczeństwem systemów informatycznych, dokumentacja powinna zawierać:

a. definicję bezpieczeństwa informacji, jego ogólne cele i zakres oraz znaczenie bezpieczeństwa jako mechanizmu umożliwiającego współużytkowanie informacji;
b. oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji;
c. krótkie wyjaśnienie polityki bezpieczeństwa, zasad, standardów i wymagań zgodności mających szczególne znaczenie dla instytucji, np.:
   - zgodność z prawem i wymaganiami wynikającymi z umów,
   - wymagania dotyczące kształcenia w dziedzinie bezpieczeństwa,
   - zapobieganie i wykrywanie wirusów oraz innego złośliwego oprogramowania,
   - zarządzanie ciągłością działania biznesowego,
   - konsekwencje naruszenia polityki bezpieczeństwa;

[34] http://www.giodo.gov.pl/1520074/j/pl/.
[35] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych…*, www.lex.pl.

d. definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania przypadków naruszenia bezpieczeństwa;
e. odsyłacze do dokumentacji mogącej uzupełniać politykę, np. bardziej szczegółowych polityk bezpieczeństwa i procedur dla poszczególnych systemów informatycznych lub zasad bezpieczeństwa, których użytkownicy powinni przestrzegać.

Zamieszczenie w polityce bezpieczeństwa wymogów określonych w Polskiej Normie nie jest obowiązkowe i zależy od decyzji administratora danych.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych jest drugim wymaganym na mocy rozporządzenia dokumentem opisującym system przetwarzania danych osobowych. Dokumentacja ta wymagana jest jednak jedynie w przypadkach administrowania danymi w systemie informatycznym. Administratorzy, którzy przetwarzają dane w sposób tradycyjny, nie muszą jej tworzyć i posiadać. Nie są także obowiązani do powołania ASI (administratora systemu informatycznego). W przepisach nie określono jednak szczegółowo zakresu obowiązków administratora bezpieczeństwa informacji. Ustawodawca ograniczył się tylko do ogólnego stwierdzenia, że administrator bezpieczeństwa informacji ma nadzorować przestrzeganie zasad ochrony, o których mowa w art. 36 ust. 1 Ustawy o ochronie danych osobowych, z czego wynika, że obowiązkiem administratora bezpieczeństwa informacji jest nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych. Administrator bezpieczeństwa informacji powinien nadzorować przede wszystkim zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem[36]. Zgodnie z § 5 rozporządzenia instrukcja zarządzania systemem informatycznym powinna zawierać w szczególności:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności;
- stosowane metody i środki uwierzytelnienia (działań, których celem jest weryfikacja deklarowanej tożsamości podmiotu) oraz procedury związane z ich zarządzaniem i użytkowaniem;
- procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;

[36] A. Drozd, *Zabezpieczenie danych osobowych*, Wrocław 2008, s. 65 i n.

- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania;
- sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe, a także kopii zapasowych;
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- sposób odnotowywania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Aby całość dokumentacji opracowanej przez rektora mogła prawidłowo funkcjonować, wymaga nie tylko ogłoszenia jako aktów prawa wewnątrzuczelnianego, ale także musi zostać właściwie wdrożona. Polityka bezpieczeństwa wprowadzana jest bowiem na mocy zarządzenia rektora, co zapewnia jej stosowne miejsce w hierarchii źródeł „prawa uczelnianego". Sam fakt obowiązywania nie oznacza jednak wdrożenia zasad przyjętych celem ochrony danych osobowych. Najistotniejszym elementem wdrożenia jest zaznajomienie z ich treścią osób upoważnionych do przetwarzania danych. Stworzenie i wdrożenie dokumentacji dotyczącej ochrony danych osobowych nie jest czynnością jednorazową[37]. Na administratorze danych osobowych ciąży bowiem obowiązek stałej aktualizacji stworzonej dokumentacji, zarówno pod kątem zmian w przepisach prawa, jak i zamian w sytuacji faktycznego przetwarzania danych osobowych (np. zmiana pomieszczeń, w których przetwarzane są dane, zmiana struktury systemu informatycznego, poprzez jego unowocześnianie, zmiana osób upoważnionych do przetwarzania danych).

Całość opublikowanej i wdrożonej dokumentacji związanej z ochroną danych osobowych w uczelni tworzy swoisty system ochrony danych. Do dokumentacji tej zaliczyć należy także wyznaczenie administratora bezpieczeństwa informacji, upoważnienia do przetwarzania danych, ewidencja osób upoważnionych do przetwarzania danych. Ewidencja osób upoważnionych do przetwarzania danych w praktyce może dzielić się na dwie odrębne ewidencje. Zgodnie z art. 39 ust. 1 Ustawy o ochronie danych w ewidencji powinny się znaleźć następujące informacje: imię i nazwisko osoby upoważ-

[37] A. Gałach, *Instrukcja ochrony danych osobowych w systemie informatycznym*, Gdańsk 2004, s. 53.

nionej; data nadania i ustania oraz zakres upoważnienia do przetwarzania danych; identyfikator, jeżeli dane są przetwarzane w systemie informatycznym. W szkołach wyższych często jednak zdarza się tak, że nie wszystkie osoby przetwarzające dane studentów przetwarzają je w systemie informatycznym. Z tego względu tworzone są dwie odrębne często ewidencje, jedna stanowiąca spis wszystkich osób posiadających upoważnienie do przetwarzania danych oraz druga będąca wykazem osób pracujących na systemach informatycznych. Zawsze jednak osoby posiadające dostęp do systemu informatycznego muszą mieć ogólne upoważnienie do przetwarzania danych. Innymi słowy, każdy pracownik uczelni przetwarzający dane studentów musi posiadać stosowne umocowanie w tym zakresie i zostać ujęty w ewidencji osób upoważnionych do przetwarzania danych, jednak nie każda z tych osób musi posiadać uprawnienie do przetwarzania danych w systemie informatycznym. Co więcej, jeżeli dostęp do danych przetwarzanych w systemie informatycznym mają co najmniej dwie osoby, dla każdej z nich powinien być zarejestrowany odrębny identyfikator, a dostęp do danych powinien być możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

Ewidencja prowadzona jest zazwyczaj w formie pisemnej. Na gruncie przepisów nie zostało jednak przesądzone, w jakiej formie powinna ona być prowadzona. Wydawałoby się, że uzasadnione jest przyjęcie rozwiązania stosowania formy pisemnej choćby ze względów dowodowych, przy czym w stosunku do osób przetwarzających dane w systemie informatycznym wystarczająca jest forma elektroniczna. Osoby te są już bowiem wymienione w ogólnej ewidencji osób upoważnionych do przetwarzania danych. Poza umocowaniem ze strony ASI muszą mieć pełnomocnictwo nadane przez administratora danych do ich przetwarzania. W konsekwencji tego osoby pracujące w systemie informatycznym już raz zostają wykazane w ewidencji prowadzonej z zachowaniem formy pisemnej.

Ewidencja osób poza funkcją rejestrową pełni także rolę porządkującą. Za pomocą ewidencji administratorzy danych osobowych w prosty sposób weryfikują pracowników posiadających dostęp do danych, choćby pod kątem zachowania przez nich tajemnicy danych.

Podsumowanie

Biorąc pod uwagę całokształt przedstawionych rozważań na temat ochrony danych osobowych w szkołach wyższych, należy podkreślić, że w stosunku do danych przetwarzanych w uczelniach stosuje się ogólne zasady wymienione w Ustawie o ochronie danych. Zgodnie z jej art. 5, ustawodawca przyjmuje zasadę rozstrzygania zbiegu norm na korzyść tych norm, które przewidują wyższy poziom ochrony. Innymi słowy, jeżeli ustawy szczególne regulują kwestie ochrony danych, zapewniając jeszcze bardziej rygorystyczne mechanizmy bezpieczeństwa, stosuje się przepisy tych ustaw. W polskim systemie prawnym istnieje relatywnie wiele przepisów odrębnych ustaw, które odnoszą się do szeroko rozumianego przetwarzania danych, przy czym znaczna ich część została wydana wcześniej niż obowiązująca Ustawa o ochronie danych osobowych. W przypadku szkół wyższych przepisy Ustawy o szkolnictwie wyższym nie regulują kwestii ochrony danych osobowych studentów. Ta swoista ochrona w każdym przypadku (nie tylko w szkołach wyższych) niesie za sobą ochronę własności osób fizycznych. W związku z tym bezpieczeństwo powinno być rozpatrywane w kontekście organizacyjnym, technicznym i prawnym. Interdyscyplinarne podejście do zagadnienia umożliwia zapewnienie wysokiego poziomu jakości wprowadzanych procedur, zwłaszcza że systemy bezpieczeństwa danych powinny być dopasowane do specyfiki działania w uczelniach.